

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-358717

(43) Date of publication of application : 26.12.2001

(51)Int.Cl.

H04L 12/24  
H04L 12/26  
G06F 13/00  
G06F 15/00  
H04L 12/46  
H04L 12/28  
H04L 12/56  
// G06F 17/60

(21)Application number : 2000-175815

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 12.06.2000

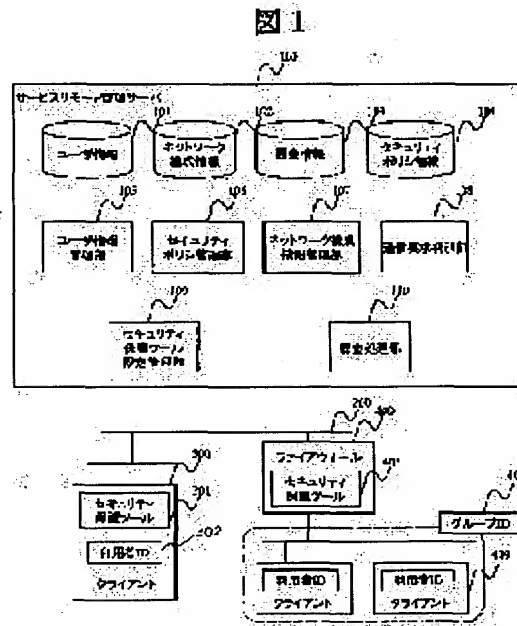
(72)Inventor : FUJI HITOSHI

**(54) METHOD AND DEVICE FOR MANAGING NETWORK DEVICE OR THE LIKE AND PROGRAM RECORDING MEDIUM**

(57)Abstract:

**PROBLEM TO BE SOLVED:** To allow a side entrusted with the management of a network, device, software, etc., to perform entrusted work and to obtain a remuneration from an entrusting side.

**SOLUTION:** In this method for managing the network device, etc., a network user transmits a communication request to a managing device such as the network device via a network, the managing device receives the communication request, changes the settings of network device software, etc., needed to meet the communication request on the basis of the received communication request, performs communication request reflection processing on the basis of a user ID or group ID attached to the communication request, performs the request reflection processing as it is in the case of a system according to weight, delivers the network device, the software, etc., whose setting has to be changed to meet the communication request from network configuration information, gives a setting change instruction to the network device, the software, etc., when the communication request coincides with a security policy or when the security policy is not checked, and performs to filling after performing a series of these pieces of processing when the user who has transmitted the communication request selects charging based on the system according to weight.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-358717

(P2001-358717A)

(43) 公開日 平成13年12月26日 (2001. 12. 26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/24		G 0 6 F 13/00	5 3 0 S 5 B 0 4 9
		15/00	3 3 0 Z 5 B 0 8 5
G 0 6 F 13/00	5 3 0	17/60	3 3 2 5 K 0 3 0
	3 3 0	H 0 4 L 11/08	5 K 0 3 3
H 0 4 L 12/46		11/00	3 1 0 C

審査請求 未請求 請求項の数12 O L (全 17 頁) 最終頁に続く

(21) 出願番号 特願2000-175815(P2000-175815)

(22) 出願日 平成12年6月12日 (2000. 6. 12)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 富士 仁

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100083552

弁理士 秋田 収喜

F ターム(参考) 5B049 AA06 CC36 GG04 GG07

5B085 ACD4 AED2 BG07

5K030 GA15 HA08 JA10 KA01 KA07

KA13

5K033 AA08 CC01 DA01 DB14 DB20

EA07

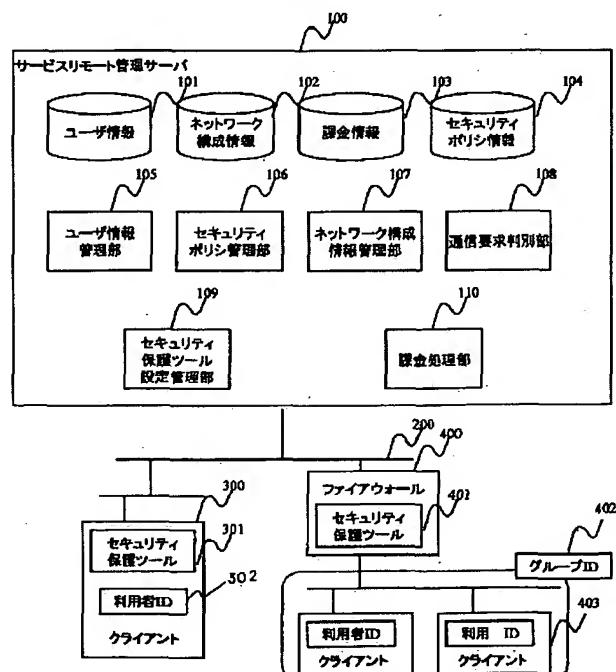
(54) 【発明の名称】 ネットワーク機器等の管理方法及び装置ならびにプログラムの記録媒体

(57) 【要約】

【課題】 ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得る。

【解決手段】 ネットワーク利用者が、通信要求をネットワーク経由でネットワーク機器等の管理装置に送信し、通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、通信要求に付与されている利用者ID又はグループIDに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うネ

図 1



## 【特許請求の範囲】

【請求項1】 ネットワークの管理を実施するユーザネットワーク機器、ソフトウェア等の設定変更を必要とするユーザのセキュリティポリシーのチェックを、マネージドサービスプロバイダ側で実施するようにすることを特徴とするネットワーク機器等の管理方法。

【請求項2】 ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、前記通信要求に付与されている利用者ID又はグループIDに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項3】 ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ID又はグループIDを付与し、前記管理装置では、送信されてきた利用者ID又はグループIDを識別し、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシーに合致しているか否かのチェックを行い、前記通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行い、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項4】 請求項2又は3に記載のネットワーク機器等の管理方法において、前記管理装置には、新規の利

とするネットワーク機器等の管理方法。

【請求項5】 請求項4に記載のネットワーク機器等の管理方法において、前記課金情報には、課金方法、決済方法などが含まれ、課金方法は、ネットワーク利用者単位、又はネットワーク利用者が属するグループ単位に、従量制課金又は定額制課金を選択可能とすることを特徴とするネットワーク機器等の管理方法。

【請求項6】 請求項5に記載のネットワーク機器等の管理方法において、ネットワーク利用者単位又はグループ単位での課金は、ネットワーク利用者が通信要求を管理装置に送信するたびに、そのネットワーク利用者が事前に登録している決済方法に対して請求処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項7】 請求項6に記載のネットワーク機器等の管理方法において、前記請求処理が、従量制課金の場合には、ネットワーク利用者の通信要求が送信されるたびに、ある金額の請求が加算される形で行われ、定額制課金の場合には、ネットワーク利用者の通信要求が送信されるときに定額制課金であるかが確認されることを特徴とするネットワーク機器等の管理方法。

【請求項8】 請求項2乃至7のうちいずれか1項に記載のネットワーク機器等の管理方法において、前記管理装置では、送信されてきた利用者ID又はグループIDを識別し、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項9】 ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、前記通信要求に付与されている利用者ID又はグループIDに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】 ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除

するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更する手順と、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ID又はグループIDを付与する手順と、前記管理装置では、送信されてきた利用者ID又はグループIDを識別する手順と、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックする手順と、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックする手順と、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシーに合致しているか否かのチェックを行う手順と、前記通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出する手順と、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項11】 サービスリモート管理サーバと、前記サービスリモート管理サーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（例えばインターネット）と、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォールとを有するネットワーク機器等の管理装置において、サービスリモート管理サーバが、利用者の情報を記録（保存）しているユーザ情報データベースと、ネットワーク構成情報を保存しているネットワーク構成情報データベースと、課金方法、決済方法及びサービスに対する課金の情報を記録（保存）している課金情報データベースと、ネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部と、通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定導出部と、ネットワーク利用者の使っているネットワークの情報を管理しているネットワーク構成情報管理部と、ネットワーク利用者から通信要求が送られて来たときに課金処理を行

機器等の管理装置。

【請求項12】 請求項11に記載のネットワーク機器等の管理装置において、前記セキュリティ保護ツール設定導出部は、利用者が登録情報をユーザ情報管理部に送信する手段と、前記送信された登録情報をユーザ情報データベース（利用者登録データベース）に記録（保存）する手段と、利用者登録が済んでからセキュリティポリシーをセキュリティポリシー管理部に送信する手段と、セキュリティポリシー情報データベースに登録する手段と、ネットワーク利用者から通信要求を受け付ける手段と、前記受け付けられた通信要求に基づくセキュリティポリシーの変更処理を行う手段とを有することを特徴とするネットワーク機器等の管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク機器、ソフトウェア等の管理をマネージドサービスプロバイダと呼ばれる外部組織に委託することに関し、特に、ネットワーク利用者が論理閉域網を要求してから、人による作業を介することなく、論理閉域網を使えるようにすると共に、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得る方法及び装置に適用して有効な技術に関するものである。

【0002】

【従来の技術】ネットワーク機器、ソフトウェア等のネットワーク管理をマネージドサービスプロバイダと呼ばれる外部組織、企業など（以下、MSPと称する）にアウトソーシングすることが行われている。これは、ある物理ネットワークに接続されているネットワーク機器、ソフトウェア等、又はある物理ネットワークと専用線などの他者と共有しないネットワークで接続されている別の物理ネットワークに設置されているある物理ネットワークの接続に使われているネットワーク機器、ソフトウェア等を、MSPがそのネットワークの所有者の要望に沿った方針で管理することによって、管理の対価を得るサービスとして行われている。

【0003】

【発明が解決しようとする課題】しかしながら、前記MSPによるネットワーク機器等の管理サービスでは、ネットワーク機器を経由する他ネットワークとの接続方針の決定は、ネットワークの所有者（個人又は組織）にあり、その方針又は具体的なネットワーク機器等の設定内容をMSPに伝えることによって、方針が伝えられたときにはMSPがネットワーク機器固有の設定情報に変換し、ネットワーク機器の設定内容が伝えられたときにはその内容を使い、ネットワーク機器の設定を行う。

【0004】このネットワークの所有者からMSPへ伝えられた方針又は設定情報は、ネットワーク所有者が保持しているセキュリティポリシーに合致していることが求

められる。このため内容のチェックが行われるのが普通で、ネットワークの所有者が行うか、チェック自体もMSPによって行われる。

【0005】このようなチェックは、これまで人の手を介するしか方法がなかったため、ネットワーク利用者の通信要求は、ネットワークの所有者、その所有者から委託されたネットワーク管理者、又はその利用者からMSPによってチェックされていた。

【0006】そこで、ネットワーク利用者の通信要求等のチェックを、人の手を介することなくMSP側で行うことができるようにすることが要望されている。

【0007】本発明の目的は、ネットワーク機器、ソフトウェア等の管理を行うネットワーク機器等の管理方法及び装置において、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得ることが可能な技術を提供することにある。

【0008】本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【0009】

【課題を解決するための手段】本願において開示される発明の概要を簡単に説明すれば、下記のとおりである。

【0010】(1) ネットワークの管理を実施するユーザネットワーク機器、ソフトウェア等の設定変更を必要とするユーザのセキュリティポリシーのチェックを、マネージドサービスプロバイダ側で実施するようにするネットワーク機器等の管理方法である。

【0011】(2) ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、前記通信要求に付与されている利用者ID又はグループIDに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うネットワーク機器等の管理方法である。

【0012】(3) ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、

ク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ID又はグループIDを付与し、前記管理装置では、送信されてきた利用者ID又はグループIDを識別し、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるかどうかをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシーに合致しているか否かのチェックを行い、前記通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うネットワーク機器等の管理方法である。

【0013】(4) 前記手段(2)又は(3)のネットワーク機器等の管理方法において、前記管理装置には、新規の利用者の登録及び課金情報について登録されるものである。

【0014】(5) 前記手段(4)のネットワーク機器等の管理方法において、前記課金情報には、課金方法、決済方法などが含まれ、課金方法は、ネットワーク利用者単位、又はネットワーク利用者が属するグループ単位に、従量制課金又は定額制課金を選択可能とするものである。

【0015】(6) 前記手段(5)のネットワーク機器等の管理方法において、ネットワーク利用者単位又はグループ単位での課金は、ネットワーク利用者が通信要求を管理装置に送信するたびに、そのネットワーク利用者が事前に登録している決済方法に対して請求処理を行うものである。

【0016】(7) 前記手段(6)のネットワーク機器等の管理方法において、前記請求処理が、従量制課金の場合には、ネットワーク利用者の通信要求が送信されるたびに、ある金額の請求が加算される形で行われ、定額制課金の場合には、ネットワーク利用者の通信要求が送信されるときに定額制課金であるかが確認される。

【0017】(8) 前記手段(2)乃至(7)のうちの

ずれか1つのネットワーク機器等の管理方法において、前記管理装置では、送信されてきた利用者ID又はグループIDを識別し、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行うものである。

【0018】(9) ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更する手順と、前記通信要求に付与されている利用者ID又はグループIDに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出する手順と、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0019】(10) ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更する手順と、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ID又はグループIDを付与する手順と、前記管理装置では、送信されてきた利用者ID又はグループIDを識別する手順と、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックする手順と、権限がある場合には、通信要求を送信した利用者又はグループ

がないことをチェックする手順と、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシーに合致しているか否かのチェックを行う手順と、前記通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出する手順と、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0020】(11) サービスリモート管理サーバと、前記サービスリモート管理サーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（インターネット）と、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォールとを有するネットワーク機器等の管理装置において、サービスリモート管理サーバが、利用者の情報を保存しているユーザ情報データベースと、ネットワーク構成情報を保存しているネットワーク構成情報データベースと、課金方法、決済方法及びサービスに対する課金の情報を保存している課金情報データベースと、ネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部と、通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定導出部と、ネットワーク利用者の使っているネットワークの情報を管理しているネットワーク構成情報管理部と、ネットワーク利用者から通信要求が送られて来たときに課金処理を行う課金処理部とを有するものである。

【0021】(12) 前記手段(11)のネットワーク機器等の管理装置において、前記セキュリティ保護ツール設定導出部は、利用者が登録情報をユーザ情報管理部に送信する手段と、前記送信された登録情報をユーザ情報データベース（利用者登録データベース）に保存する手段と、利用者登録が済んでからセキュリティポリシーをセキュリティポリシー管理部に送信する手段と、セキュリティポリシー情報データベースに登録する手段と、ネットワーク利用者から通信要求を受け付ける手段と、前記受け付けられた通信要求に基づくセキュリティポリシーの変更処理を行う手段とを有するものである。

【0022】すなわち、本発明のポイントは、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するネットワーク機器の設定を変更する要求をネット



ワーク経由で送信し、その通信要求をネットワーク機器等の管理装置（MSP側の管理装置）が受信し、受信した通信要求に基づいて前記ネットワーク機器等の管理装置（以下、単に管理装置と称する）が通信要求を満たすために必要なネットワーク機器、ソフトウェア等の設定を変更する。

【0023】このために、前記管理装置に通信要求を送るネットワーク利用者には、その利用者を一意に識別できる利用者IDを付与する。この利用者IDは、その利用者を含む一人以上が属するグループを一意に識別できるグループIDと関連付け、利用者IDからグループIDが導出できるような関係を明確にする。これらのID付与と関連付けは、新規の利用者が前記管理装置に利用者登録する際に行われる。また、この利用者登録の際に、課金情報についても登録する。

【0024】課金情報には、課金方法、決済方法などが含まれる。課金方法は、ネットワーク利用者単位、又はネットワーク利用者が属するグループ単位に、従量制課金又は定額制課金を選択可能とする。ネットワーク利用者単位での課金は、ネットワーク利用者が通信要求を前記管理装置に送信するたびに、そのネットワーク利用者が事前に登録している決済方法に対して請求処理を行い、グループ単位の課金では、ネットワーク利用者が通信要求を前記管理装置に送信するたびに、そのネットワーク利用者が属するグループが事前に登録している決済方法に対して請求処理を行う。この請求処理が、従量制課金の場合には、ネットワーク利用者の通信要求が送信されるたびに、ある金額の請求が加算される形で行われ、定額制課金の場合には、ネットワーク利用者の通信要求が送信されるときに定額制課金であることが確認される。

【0025】ネットワーク利用者が前記管理装置に送る通信要求には、利用者ID又はグループIDを付与する。どの情報を付与するかは、MSPが実施する課金方法又はMSPがネットワーク利用者単位課金もグループ単位課金も実施している場合には利用者が選択した課金方法とその管理装置が採用しているID体系に関わる。

【0026】前記管理装置では、送信されてきた利用者ID又はグループIDを識別し、それらのIDが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックする。

【0027】権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う。

【0028】前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が前記管理装置に登録されている通信要求を送信した利用者もしくは利用者が属して

かのチェックを行う。セキュリティポリシーとのチェックを行い、かつ通信要求がセキュリティポリシーに合致しているとき、又はセキュリティポリシーのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与える。これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う。

【0029】前記手段によれば、ネットワーク利用者が論理閉域網を要求してから、人による作業を介することなく、論理閉域網を使えるようになる。これにより、従来の人を介した論理閉域網の管理サービスに比べて時間を短縮することができる。

【0030】また、包含関係IDを利用することによって、サービス提供側で利用者IDとグループIDというような複数種類のIDの対応関係を表す情報を保持する必要がなくなる。

【0031】また、ネットワーク機器、ソフトウェア等の管理を行うネットワーク機器等の管理方法及び装置において、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得ることができる。

【0032】以下に、本発明について、本発明による実施形態（実施例）とともに図面を参照して詳細に説明する。

【0033】

【発明の実施の形態】まず、本発明に係るセキュリティポリシー管理方法及び装置の実施形態について説明する。

【0034】図2は、本発明に係る一実施形態のコンピュータシステムからなるセキュリティポリシー管理装置の概略構成を示す模式図である。図2において、11はネットワーク利用者からの通信要求を受け付ける第1のインタフェース、12はネットワーク管理者がセキュリティポリシーを管理する第2のインタフェース、13はセキュリティポリシー管理装置からネットワーク機器等に設定を行う第3のインタフェース、14は他セキュリティポリシー管理装置へのセキュリティポリシー登録を行うセキュリティポリシー連結部、21はネットワーク利用者からの通信要求をチェックする通信要求チェック部、22は通信要求を実現するために使える手段を検索する論理閉域網生成手段検索部、23は論理閉域網生成手段検索部22で複数の結果が検索された場合に一つの手段を選択する論理閉域網生成手段選択機構部、24は論理閉域網生成手段選択機構部23の結果に基づいて現在のネットワーク機器、ソフトウェア等に設定されている状態をチェックするセキュリティ保護ツール設定チェック部（ネットワーク機器設定チェック部）である。

【0035】30はセキュリティポリシーを保存しているセキュリティポリシーデータベース（データベース部）で

あり、このセキュリティポリシーデータベース30には、論理閉域網の状態を管理する論理閉域網構成要素管理部31、ネットワーク管理者によって管理されているセキュリティポリシー構成要素管理機構部32、及びセキュリティ保護ツールの状態を管理しているセキュリティ保護ツール構成要素管理部33を有している。

【0036】図3は、本実施形態のセキュリティポリシー管理装置の動作手順を示す流れ図である。まず、ネットワーク管理者が管理対象範囲のセキュリティポリシーを決め、それをセキュリティポリシー管理装置に登録する(S31)。このセキュリティポリシーは必要に応じて、ネットワーク管理者が追加、修正、又は削除することができる。この状態以降は、ネットワーク利用者による通信要求を受け付け(S32)、それをネットワーク機器等に設定することによって(S33)、ネットワーク利用者の要求する通信を実現する。

【0037】図4は、前記図2に示すセキュリティポリシー管理装置の動作手順の最初であるネットワーク管理者によるセキュリティポリシー管理の処理手順を示す流れ図である。第2のインターフェース(セキュリティポリシー管理インタフェース)12から入力されたセキュリティポリシーは、図4に示すように、追加、変更、又は削除の処理が行われ(S41、S42、S43)、その結果は、セキュリティポリシー構成要素管理部32に保存される(S44)。

【0038】図5は、セキュリティポリシー管理装置の動作手順(図3)のネットワーク利用者による通信要求処理と、セキュリティポリシー管理装置による機器設定処理の両者に関わる処理手順を示している。これらの処理は、ネットワーク利用者の通信要求が、第1のインターフェース(ユーザ要求インタフェース)11から入力されたことにより削除の場合は、通信要求チェック部21は、要求時点に存在している論理閉域網の情報を論理閉域網構成要素管理部31から得る。

【0039】図5に示すように、入力された通信要求が、要求を受け付けたセキュリティポリシー管理装置1000の管理対象範囲内の要求か、他セキュリティポリシー管理装置2000の管理対象範囲に属する機器との通信が含まれるかという管理対象チェックを、通信要求チェック部21が、セキュリティポリシー構成要素管理部32に対して行う(S51)。この結果、他セキュリティポリシー管理装置にセキュリティポリシーを管理されている機器との通信要求が含まれている場合(NG)、その管理装置2000を特定し、特定した管理装置2000のセキュリティポリシー連結部2001に対して、セキュリティポリシー連結部14からセキュリティポリシーの問い合わせを行う(S52)。

【0040】これとは別に、通信要求がセキュリティポリシー管理装置1000のセキュリティポリシーの範囲内で

セキュリティポリシー構成要素管理部32で行う(S53)。セキュリティポリシー管理装置1000で通信要求がセキュリティポリシーの範囲内であることが確認され、同時に、セキュリティポリシー管理装置2000でも通信要求がセキュリティポリシーの範囲内であることが確認され(OK)、その結果をセキュリティポリシー管理装置1000が受け取った場合は、機器設定処理を行う(S54)。また、いずれか一方のセキュリティポリシー管理装置でセキュリティポリシーに合わない通信要求である(NG)ことが明らかになった場合には、そこで通信要求を実現するための処理は中断し、通信要求を出したネットワーク利用者に対してメッセージで通知して(S55)処理を終了する。

【0041】前記機器設定処理(S54)では、セキュリティポリシー管理装置1000の管理対象範囲に存在する要求された通信を実現するために必要なネットワーク機器、ソフトウェア等を、論理閉域網生成手段検索部22が、セキュリティポリシー構成要素管理部32から検索する(S56)。この検索結果が、単数の場合(OK)は、その結果を用い、複数の場合(OK)は、論理閉域網生成手段選択部23において、生成手段を登録時に手段毎に付与しておいたツールの評価項目、例えば、セキュリティ強度等を利用して一種類に絞込んだ結果を用い、セキュリティ保護ツール設定チェック部24が、セキュリティ保護ツール構成要素管理部33で、その時点の機器設定情報を収集し、その設定状態と矛盾がなければ、第3のインターフェース(ネットワーク機器制御インタフェース)13から機器設定エージェント41に設定情報を渡して、機器設定エージェント41が必要な機器の設定処理を行うと共に、設定した情報を論理閉域網構成要素管理部31及びセキュリティ保護ツール構成要素管理部33に保存する。

【0042】次に、セキュリティポリシー管理装置2000の管理対象範囲に属する機器との通信が必要な場合(NG)には、セキュリティ保護ツール設定チェック部24が、セキュリティポリシー連結部14から、セキュリティポリシー連結部2001へ機器設定依頼を通知する(S57)。セキュリティポリシー管理装置2000は、この設定依頼を受け、セキュリティポリシー管理装置2000の管理範囲内にあるネットワーク機器、ソフトウェア等に設定処理を行って通信要求処理と機器設定処理を終了する。

【0043】前記通信要求チェック部21の処理は、図6に示すように、まず、通信要求の種別は、論理閉域網の変更又は削除であるかをチェックする(S60)。この結果、通信要求の種別が論理閉域網の変更又は削除であった場合は、論理閉域網構成要素管理部31から論理閉域網情報を取得する(S61)。次に、通信要求に含まれる通信要求範囲をチェックする(S62)。そのチェック結果、通信要求が自装置管理対象範囲内であれ



ば、自装置のセキュリティポリシーの検索を行い（S63）、通信要求が自装置管理対象範囲外にも跨る場合は、セキュリティポリシー連結処理を行い（S64）、次のステップS65に移る。ステップS65では通信要求がセキュリティポリシーの範囲内にあるかをチェックし、前記通信要求がセキュリティポリシーの範囲内にあれば（OK）、機器設定処理を行い（S66）、前記通信要求がセキュリティポリシーの範囲外にあれば（NG）、通信要求の否決をユーザに通知して（S67）、通信要求チェックの処理は終了する。

【0044】前記セキュリティポリシー連結の処理は、図7に示すように、他のセキュリティポリシー管理装置2000を特定し（S71）、通信要求内容を他のセキュリティポリシー管理装置2000へ通知する（S72）。次に、セキュリティポリシーチェック結果を受信し（S73）、セキュリティポリシー連結の処理を終了する。

【0045】前記機器設定処理は、図8に示すように、論理閉域網生成手段を検索し（S81）、この検索された論理閉域網生成手段のうちから所定の論理閉域網生成手段を選択し（S82）、その選択された論理閉域網生成手段は、設定に矛盾しないかチェックする（S83）。設定に矛盾しない（OK）時は、機器設定エージェントによる機器の設定を行い（S84）、その機器設定情報の保存を行う（S85）。設定に矛盾がある（NG）時は、矛盾発生メッセージを表示し（S88）、機器設定処理は終了する。

【0046】次のステップS86で通信要求範囲のチェックを行い、前記通信要求が自装置管理対象範囲外にあれば、他装置への機器の設定依頼し（S87）、前記機器設定情報が自装置管理対象範囲内にあれば、機器設定処理は終了する。

【0047】前記論理閉域網生成手段の検索処理は、図9に示すように、通信要求に含まれる端末を導出し（S91）、その導出された端末に許可されている手段を検索し（S92）、論理閉域網生成手段の検索処理は終了する。

【0048】前記論理閉域網生成手段の選択処理は、図10に示すように、論理閉域網生成手段の選択し（S101）、選択された論理閉域網生成手段は複数かをチェックし（S102）、複数であれば（Yes）、論理閉域網生成手段毎に登録されている評価項目から最良の手段を選択して（S103）、論理閉域網生成手段を選択する（S104）。前記選択された論理閉域網生成手段に基づいて論理閉域網を構築することができる。つまり、従来通りにセキュリティポリシーを保った論理閉域網を作り出すことができる。

【0049】図1は、本発明による一実施形態のネットワーク機器等の管理装置の概略構成を示すブロック構成図である。図1において、100はサービスリモート管

情報データベース（利用者登録データベース）、102はネットワーク構成情報を保存しているネットワーク構成情報データベース、103は課金方法、決済方法及びサービスに対する課金の情報を保存している課金情報データベース、104は利用者のセキュリティポリシー情報を保存しているセキュリティポリシー情報データベース、105はユーザ情報管理部、106はセキュリティポリシー管理部、107はネットワーク利用者の使っているネットワークの情報を保存しているネットワーク構成情報管理部、108はネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部、109は通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定管理部、110はネットワーク利用者から通信要求が送られて来たときに課金処理を行う課金処理部、200はリモート管理サービスサーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（例えばインターネット）、300はネットワーク利用者が使用中の個別のクライアント、400はネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォール、402は一つ以上のネットワーク利用者をまとめて管理するためのグループIDである。

【0050】本実施形態のネットワーク機器等の管理装置は、図1に示すように、サービスリモート管理サーバ100と、リモート管理サービスサーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（例えばインターネット）200と、ネットワーク利用者が使用中の個別のクライアント300と、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォール400とで構成されている。

【0051】前記サービスリモート管理サーバ100は、利用者の情報を保存しているユーザ情報データベース（利用者登録データベース）101、ネットワーク構成情報を保存しているネットワーク構成情報データベース102、課金方法、決済方法及びサービスに対する課金の情報を保存している課金情報データベース103、別のセキュリティポリシー管理装置からの利用者のセキュリティポリシー情報を保しているセキュリティポリシー情報データベース104、前記ユーザ情報データベース101からのユーザ（利用者）情報の管理を行うユーザ情報管理部105、前記利用者のセキュリティポリシー情報の管理を行うセキュリティポリシー管理部106、ネットワーク利用者の使っているネットワークの情報を保存しているネットワーク構成情報管理部107、ネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部108、通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定管理部109及びネットワーク利用者

から通信要求が送られて来たときに課金処理を行う課金処理部110を有している。

【0052】前記ネットワーク利用者が使用中の個別のクライアント300には、セキュリティ保護ツール301と利用者ID302を有している。前記ファイアウォール400は、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御する。このファイアウォール400にはグループID402が入力される。前記グループID402は、複数のクライアントの利用者ID403をまとめた識別子である。

【0053】図11は、図1のネットワーク機器等の管理装置における、ネットワーク管理委託処理手順の全体を示す流れ図である。まず、利用者が登録情報をユーザ情報管理部105に送信し、その結果をユーザ情報データベース（利用者登録データベース）101に登録（保存）し（S101）、利用者登録が済んでからセキュリティポリシーをセキュリティポリシー管理部106（図2参照）に送信し、この送信されてきたセキュリティポリシーをセキュリティポリシー情報データベース104に登録（保存）する（S102）。この状態になると、ネットワーク利用者から通信要求を受け付けることができるようになる（S103）。前記ステップS102、S103を繰り返しネットワーク管理の委託サービスが続けることができる。また、セキュリティポリシーの変更がある際には、セキュリティポリシー管理部106でセキュリティポリシーの変更処理を行ってセキュリティポリシー情報データベース104の内容を変更することもできる（図2、図6参照）。

【0054】図12は、利用者登録処理の手順を示す流れ図である。利用者登録処理には、ネットワーク情報の登録があり、どのクライアント300に何のセキュリティ保護ツール301が装備されているのか、どのファイアウォール400に何の機能が装備されているのか、といった内容をネットワーク構成情報管理部107に通知し、ネットワーク構成情報管理部107はネットワーク構成情報データベース102に登録（保存）する（S201）。次に、利用者登録しようとしている利用者は、課金方法と決済方法をユーザ情報管理部105に送信し、ユーザ情報管理部105ではその選択された課金方法（S202）と決済方法を課金情報データベース103に登録する（S203）と共に、ユーザ情報データベース101を参照し既存の利用者と一意に区別できる利用者ID302及びグループIDを生成した後に利用者に通知し（S204）、それらのID情報をユーザ情報データベース101に登録（保存）する。また、利用者には、様々な権限を表す属性を付与することができ、利用者が希望する場合には、その属性もユーザ情報データベース101に登録（保存）する。この属性には、例えば、通信要求を出すことができるユーザに付与する属

変更も行うことができるユーザに付与する属性等がある。

【0055】図13は、セキュリティポリシー登録・変更処理の手順を示す流れ図である。セキュリティポリシー登録・変更処理では、ユーザはクライアント300からセキュリティポリシーをセキュリティポリシー管理部106に送信し、セキュリティポリシー管理部106では送信されてきたセキュリティポリシーを受け付け（S301）、その受け付けたセキュリティポリシーについて、そのユーザに関するセキュリティポリシー全体としての整合性をチェックし（S302）、そのチェックで整合性が保たれていることが確認される（図2参照）と、セキュリティポリシー情報データベース104に登録（保存）する（S304）。

【0056】図14は、通信要求受付処理の手順を示す流れ図である。通信要求受付処理は、通信要求判別部108がネットワーク利用者からの通信要求を受け付けることから始まる（S401）。次に、図15に示す利用者権限チェック処理を行う（S402）。ここでは、まず、通信要求受付処理がネットワーク利用者から受け取った通信要求に含まれているグループIDやユーザIDとユーザ情報データベース101を使い、通信要求を送信する権限があるユーザからの通信要求であるか否かをチェックする（S501）。この結果、通信要求を出す権限を持った利用者からの通信要求であることが確認できれば（Yes）、次に、課金情報データベース103を使い課金方法のチェックを行う（S502）。また、権限があることが確認できない場合（S501のNo）にはサービスを拒否する（S505）。ここでは、通信要求を送信してきた利用者が課金情報データベース103に登録している課金方法から、従量制課金を選択しているか定額制課金を選択しているかを調べ、従量制課金を選択している場合は、通信要求に基づくサービスを提供した後に課金するための情報を一時的に保持する（S503）。課金方法がいずれの場合でも、さらに課金情報データベース103を使い料金の滞納があるか否かを調べ（S504）、滞納があれば（No）、サービスを拒否し（S505）、滞納が無ければ（Yes）、利用者権限チェックを終了する。

【0057】図16は、通信要求反映処理の手順を示す流れ図である。まず、通信要求判別部108が受信した通信要求が、事前に登録されているセキュリティポリシー情報データベース104に合致しているか否かを判断する（S601）。通信要求判別部108は、合致していない場合（No）はサービスを中止し（S607）、合致している場合は通信要求を実現するために設定しなければならないネットワーク機器などをネットワーク構成情報データベース102を用いて導出する（S603）。

【0058】セキュリティ保護ツール設定管理部109

は、通信要求判別部108が設定対象として導出した機器、ソフトウェア等の設定内容を個別に導出し、導出した設定内容をネットワーク機器、ソフトウェア等に対して設定する指示を与える(S604)。通信要求やネットワーク構成によって設定対象や内容は変化するが、例えば、300クライアントのように、クライアント自身にセキュリティ保護ツール301が実装されている場合には、そのツールの設定を変更し、クライアントが保持している利用者IDに対して課金処理を行うような形態もあれば、クライアントの利用者ID403が通信要求を送信した結果、外部ネットワークとの接続機器であるファイアウォール400に具備されているセキュリティ保護ツール401の設定を変更した後に、通信要求を送信したクライアントの利用者ID403が含まれるグループID402に課金する形態もあり得る。

【0059】このような設定が終わった後、課金方法を調べて(S605)、一時的に保存していた情報を基に、課金処理部110が課金処理を実施する(S606)。

【0060】図17は、通信要求を送信するクライアントで行われる通信要求送信処理の手順を示す流れ図である。クライアント300では通信要求の送信を行うソフトウェアで通信要求を入力し(S701)、利用者登録をした際の課金形態に対応する利用者ID又はグループIDを入力した通信要求に付加し(S702、S703、S704)、サービスリモート管理サーバ100へ通信要求とIDを送信する(S705)。

【0061】図18は、本サービスを利用する際に利用できるグループ課金の処理を簡略化する包含関係IDを示す図である。利用者IDは、ネットワーク利用者が通信要求を前記管理装置に送信するクライアント300に対して付与されている。利用者がクライアント300を移動することを考慮して、クライアント300へのログイン時に付与することも可能であり、特定のハードウェアに固定的に付与することも可能である。また、グループIDは、一つ以上の利用者IDの集合に対して付与される。前記図1の本実施形態では特定のサブネットに属する利用者に付与されたIDの集合を表すIDとして定義している。ネットワーク利用者単位課金の場合には利用者ID、グループ単位課金の場合には利用者IDまたはグループIDのいずれか一方を通信要求に付与する。

【0062】利用者IDとグループIDとの対応関係は、その対応情報を通信要求の受信者である前記管理装置が保持するか、包含関係を表すID体系を利用して表す。前者は、利用者IDとグループIDの対応関係を表す情報をサーバで保持する必要があるが、以下に説明する包含関係IDではそれが不要になる。包含関係IDとは、二桁以上からなる数値を固定的な桁数で分割して認識するルールをIDの送信者と受信者が予め決めてお

ことによって、利用者とグループの特定情報が交換できるものである。図18では、「000」という値を利用者個別IDに利用せず、「000」がついている場合にはグループIDを表すというルールにしておくことによって、包含関係IDが達成されている。

【0063】なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。

【0064】また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ROM、CD-ROM等の記録媒体、コンピュータシステムに内蔵されるハードディスク等の記録装置をいう。

【0065】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【0066】

【発明の効果】以上説明したように、本発明によれば、ネットワーク利用者が論理閉域網を要求してから、人による作業を介することなく、論理閉域網を使えるようになるので、人を介した論理閉域網の管理サービスに比べて時間を短縮することができる。

【0067】また、包含関係IDを利用することによって、サービス提供側で利用者IDとグループIDというような複数種類のIDの対応関係を表す情報を保持する必要がなくなる。

【0068】また、ネットワーク機器、ソフトウェア等の管理を行うネットワーク機器等の管理方法及び装置において、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得ることができる。

【図面の簡単な説明】

【図1】本発明による一実施形態のネットワーク機器等の管理装置の概略構成を示すブロック構成図である。

【図2】本発明に係る一実施形態のコンピュータシステムからなるセキュリティポリシ管理装置の概略構成を示すブロック構成図である。

【図3】図2に示すセキュリティポリシ管理の処理手順を示す流れ図である。

【図4】図2に示す機器設定処理の処理手順を示す流れ図である。

【図5】図3に示す通信要求処理手順を示す流れ図である。

【図6】本実施形態の通信要求チェック部の処理手順を示す流れ図である。

【図7】本実施形態のセキュリティポリシ連結の処理手順を示す流れ図である。

【図8】本実施形態の機器設定処理の手順を示す流れ図

である。

【図9】本実施形態の論理閉域網生成手段の検索処理手順を示す流れ図である。

【図10】本実施形態の論理閉域網生成手段の選択処理手順を示す流れ図である。

【図11】本実施形態のネットワーク管理委託処理手順の全体を示す流れ図である。

【図12】本実施形態の利用者登録の処理手順を示す流れ図である。

【図13】本実施形態のセキュリティポリシー登録・変更処理手順を示す流れ図である。

【図14】本実施形態の通信要求受付処理手順を示す流れ図である。

【図15】本実施形態の利用者権限チェック処理手順を示す流れ図である。

【図16】本実施形態の通信要求反映処理手順を示す流れ図である。

【図17】本実施形態の通信要求送信処理手順を示す流れ図である。

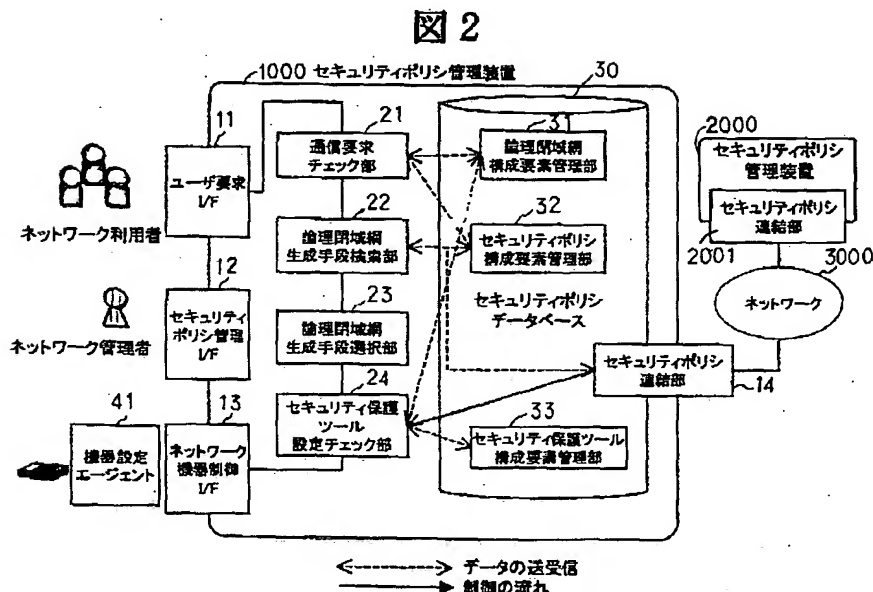
【図18】本実施形態の包含関係IDの例を示す図である。

【符号の説明】

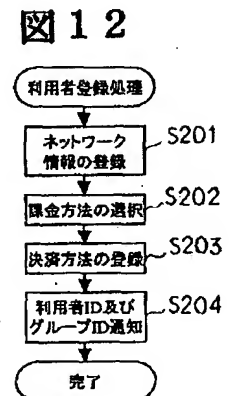
- 11…第1のインタフェース
- 12…第2のインタフェース
- 13…第3のインタフェース
- 14…セキュリティポリシー連結部
- 21…通信要求チェック部
- 22…論理閉域網生成手段検索部
- 23…論理閉域網生成手段選択部
- 24…セキュリティ保護ツール設定チェック部

- 24…セキュリティ保護ツール設定チェック部
- 30…セキュリティポリシーデータベース
- 31…論理閉域網構成要素管理部
- 32…セキュリティポリシー構成要素管理部
- 33…セキュリティ保護ツール構成要素管理部
- 41…機器設定エージェント
- 1000…セキュリティポリシー管理装置
- 2000…セキュリティポリシー管理装置
- 2001…セキュリティポリシー連結部
- 100…サービスリモート管理サーバ
- 101…ユーザ情報データベース
- 102…ネットワーク構成情報データベース
- 103…課金情報データベース
- 104…セキュリティポリシー情報データベース
- 105…ユーザ情報管理部
- 106…セキュリティポリシー管理部
- 107…ネットワーク構成情報管理部
- 108…通信要求判別部
- 109…セキュリティ保護ツール設定管理部
- 110…課金処理部
- 200…ネットワーク
- 300…クライアント
- 301…セキュリティ保護ツール
- 302…利用者ID
- 400…ファイアウォール
- 401…セキュリティ保護ツール
- 402…グループID
- 403…クライアントの利用者ID

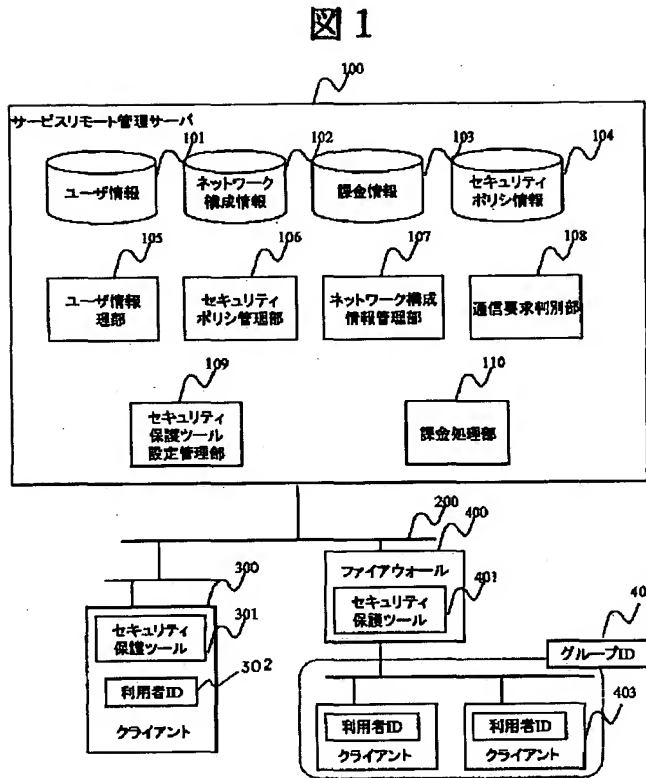
【図2】



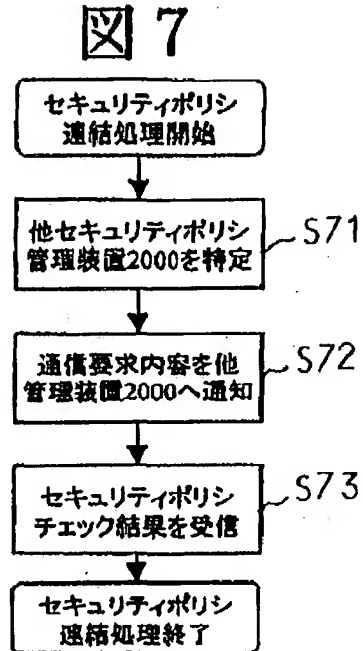
【図12】



【図1】

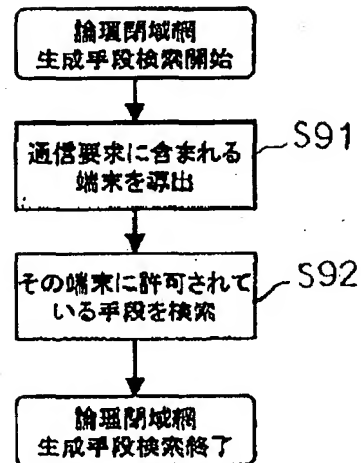


【図7】



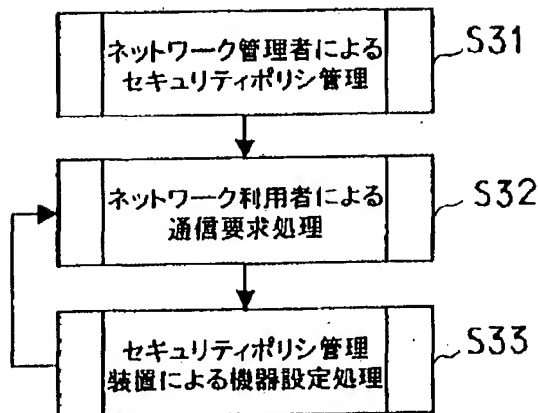
【図9】

図9

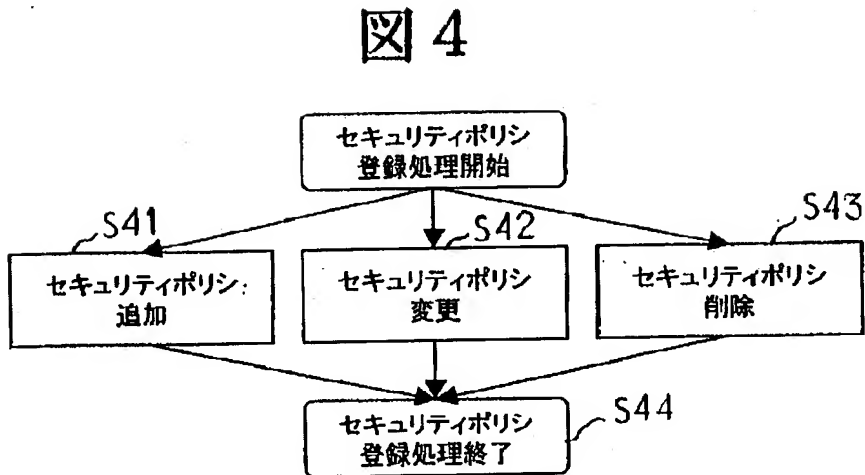


【図3】

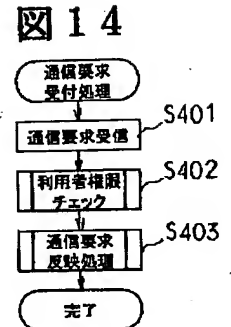
図3



【図 4】

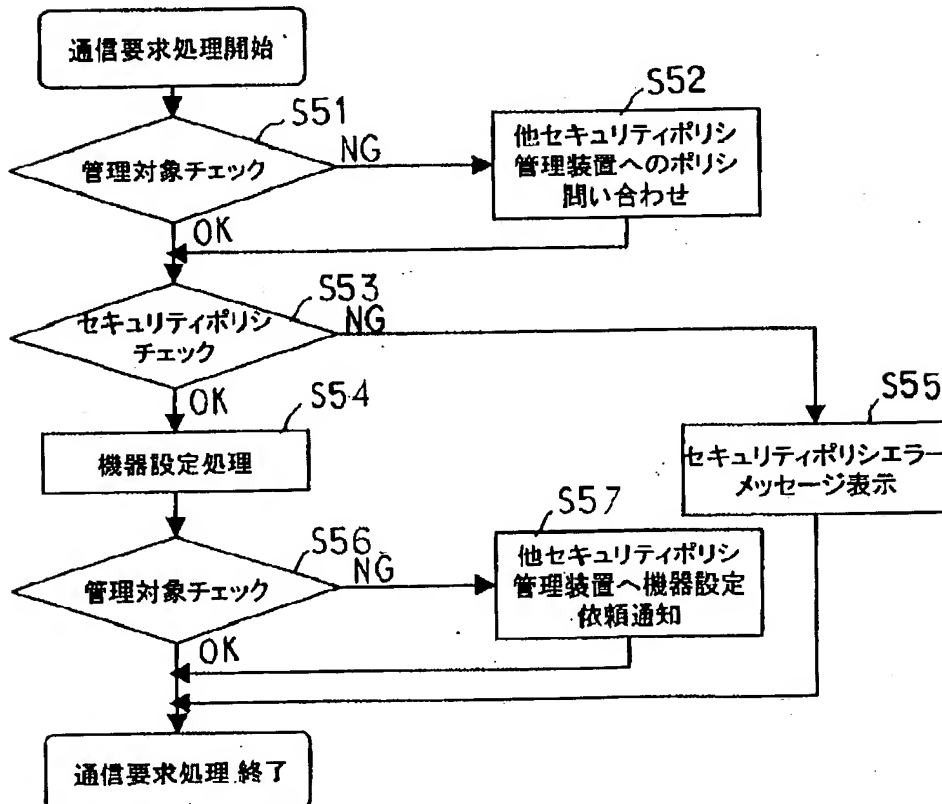


【図 14】



【図 5】

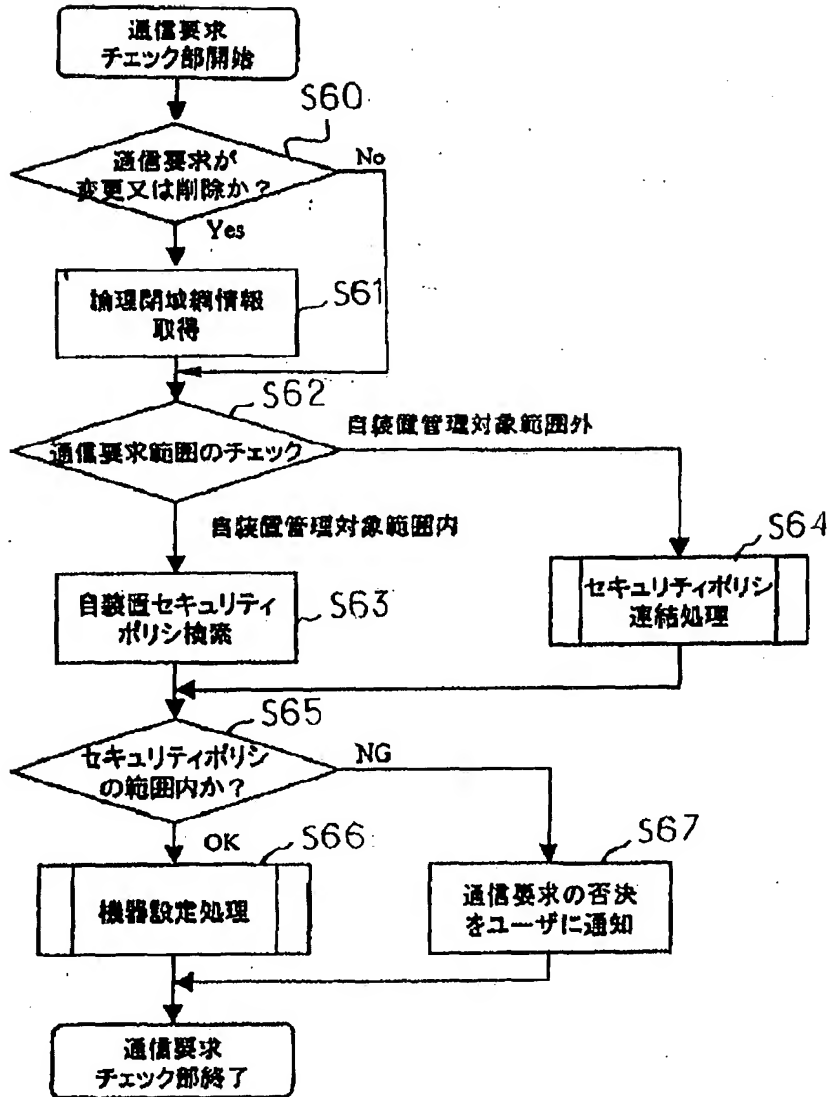
**図 5**





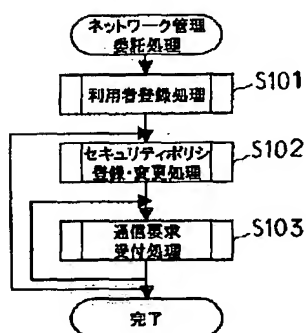
【図6】

図 6



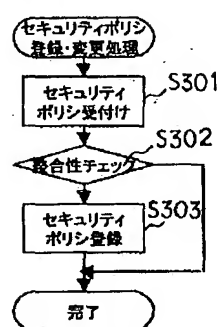
【図11】

図 1 1

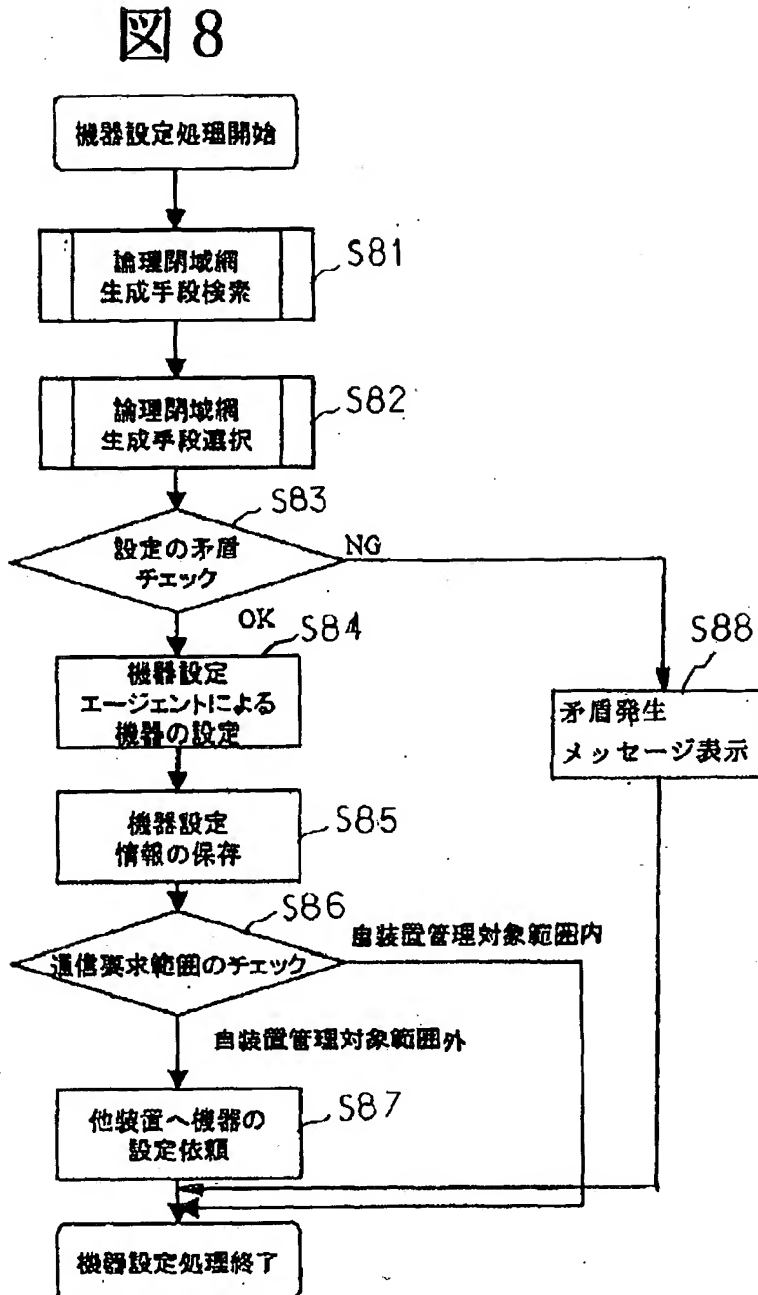


【図13】

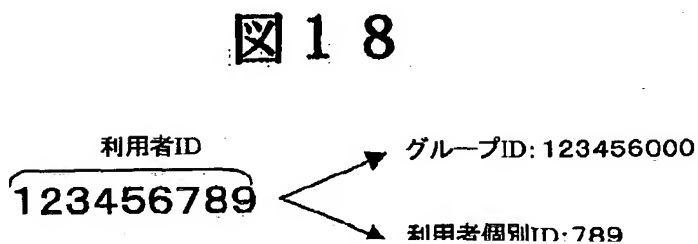
図 1 3



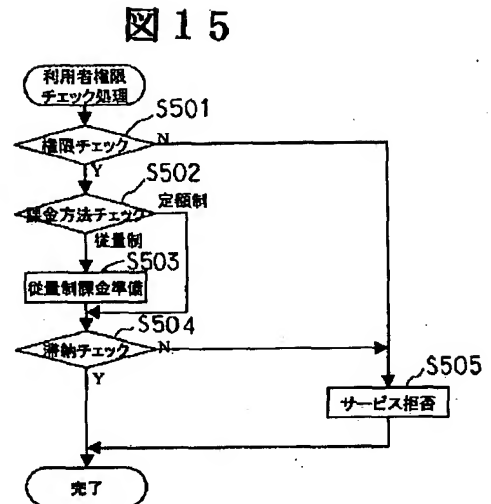
【図8】



【図18】

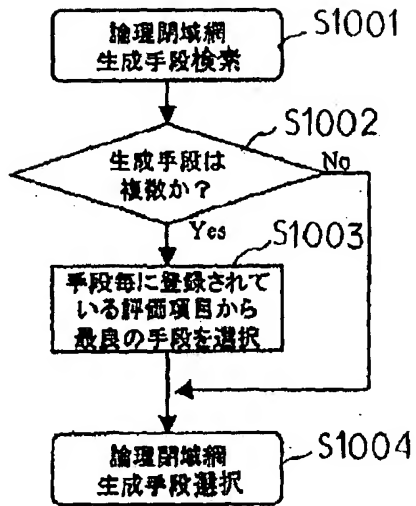


【図15】



【図10】

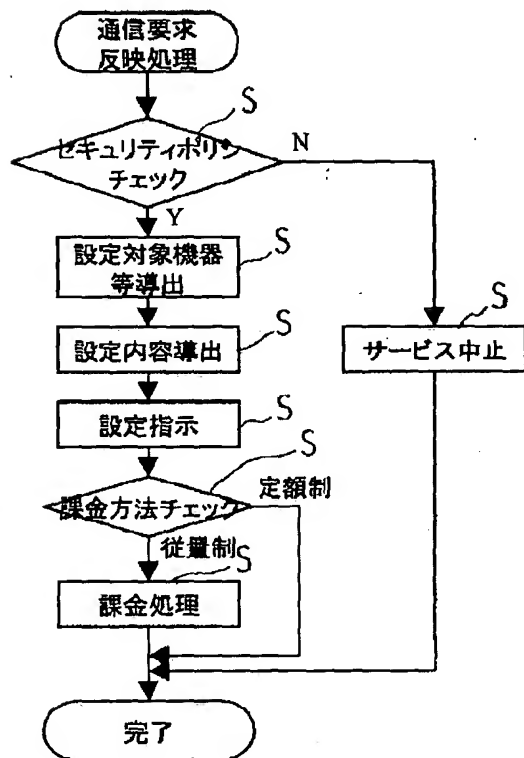
# 図 1 0



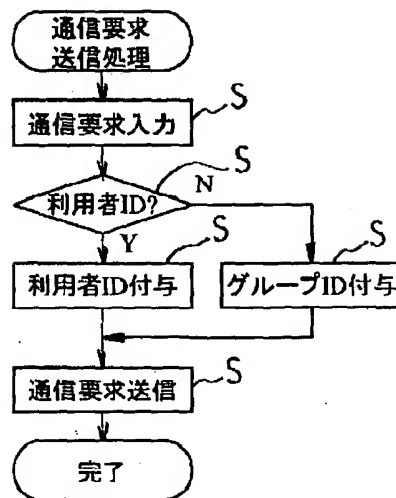
【図16】

【図17】

# 図 1 6



# 図 1 7



フロントページの続き

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テ-マ-ド (参考)
H 0 4 L 12/28		H 0 4 L 11/20	1 0 2 D
12/56			
// G 0 6 F 17/60	3 3 2		